REMARKS

Claims 55-91 remain in this application. Original Claims 1-54 have been cancelled. No new matter has been added. Applicants respectfully request reconsideration and review of the application in view of the following remarks.

Applicants acknowledge with appreciation the courtesy of the Examiner in conducting the telephonic interviews on May 24 and 27, 2005. In the interviews, the Examiner acknowledged that the amended claims were distinguishable over the references of record.

The Examiner rejected Claim 18 under 35 U.S.C. § 112, second paragraph, as indefinite. In view of the cancellation of this claim, this ground of rejection is deemed moot.

The Examiner rejected Claims 1-8, 10-12, 14-35, 37-39, and 41-54 as conflicting with Claims 1-42 of copending application Serial No. 09/904,962 and Claims 1-50 of copending application Serial No. 09/992,378. Without commenting on the merits of this rejection, Applicants note that the original claims of this application have all been cancelled and that none of the currently presented claims in this application are in conflict with any of the claims of the two referenced copending applications.

The Examiner also provisionally rejected certain claims of this application under the judicially created doctrine of obviousness-type double patenting as unpatentable over the two referenced copending applications. While Applicants consider the claims of this application to be patentably distinct over the claims of the two referenced copending applications, Applicants will submit a Terminal Disclaimer to obviate this ground of rejection should it be maintained by the Examiner.

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the invention. The patent application is generally directed to a location-based method of controlling access to digital information. In an embodiment of the invention, the digital information is encrypted using an encryption key based on a location value that identifies a specific geographic

location at which access to the digital information is authorized. The encryption key may be further based on an area parameter that is determined from the location value and is appended to the encrypted digital information. The area parameter describes a shape of a geographic area, but does not identify where the geographic area is located. The device that receives the encrypted digital information can generate a decryption key to decrypt the digital information based on the received area parameter and the location determined by the device. If the device location is not within the proximate area defined by the location value, the device will be unable to generate a decryption key to decrypt the digital information. Thus, the integrity of the digital information is protected.

The Examiner rejected all of the claims under various combinations of Shimada, Laurance et al., Schipper, Fennel, Jr. et al., Hastings and Emery et al. In view of the cancellation of the original claims, these grounds of rejection are considered moot. Applicants further consider the references inapplicable to the claims presented in this Amendment.

Shimada discloses a data processing method in which access to information is controlled using a password and location attribute data. A data file includes fields for the storing of attributes defining a password and location. When it is desired to access the data file, a data processing system compares the stored password to one inputted by a user, and also compares the stored location data to a current location determined by a location determining system (e.g., GPS). If the password is correct and the location matches, then access to the data file is permitted. In this regard, Shimada provides a mere gatekeeper function in allowing/disallowing access to information. The attribute data is added to the control structure for the data files, but does not alter or transform the data in any respect. Instead, the attribute data provides only an arbitrary linkage with the data files. Once the data files are accessed, the information can be freely disseminated, i.e., copied, stored, displayed, transmitted, etc., because the arbitrary linkage between the data files and the location information ends.

As a result, Shimada provides no ability to limit access to the stored information

at the specific geographic location. Shimada does not encrypt the data using location information, nor does Shimada disclose anything corresponding to the "area parameter" as that term is described in the specification and used in the claims. Shimada therefore fails to suggest or disclose any claim of the patent application.

Laurance et al. discloses a satellite communication system that is used for authenticating messages between a transmitter and a receiver. The sender of a message formulates the message and may encrypt it using a key that depends on position and non-position elements. The position elements may include the location of the sender or the receiver. The encrypted message is sent to a satellite, which determines the location of the sender and appends that information to the message. The message is then forwarded to the receiver with the appended location information. The receiver then receives the message and extracts the satellite-appended location information. The receiver compares the appended location information to data previously saved in memory. If the location information matches, then the message is authenticated and the message is decrypted using the previously stored (or satellite provided) data. If the location information does not match, then the message is assumed to be bogus and not acted upon.

There are several distinctions between Laurance and the present invention. First, Laurance discloses a communication system in which messages are sent between trusted users, and the purpose of the reference is to authenticate their communications. The satellite serves as a trusted intermediary between the sender and receiver, and is necessary to verify the location of the sender or receiver to authenticate the message. In contrast, the present invention may facilitate communications between any two users as long as the sender knows the location of the receiver. No trusted intermediary is required. Second, Laurance fails to disclose anything corresponding to an "area parameter" as that term is described in the specification and used in the claims. Third, the receiver in Laurance does not determine its own location, but rather is provided that information by a third party (i.e., the satellite). The receiver is therefore

reliant upon the third party to authenticate the message. For these and other reasons, Laurance fails to suggest or disclose any claim of the present application.

Schipper discloses a method of communicating between mobile stations using present and past location information to vary an encryption key. The mobile stations each have a satellite positioning system (SATPS) receiver and antenna that receive signals from a plurality of navigation satellites. The SATPS receiver generates psuedorange measurements from that station to each navigation satellite in view, and produces location information based on a plurality of pseudorange measurements. Schipper periodically communicates pseudorange correction values (PRC) from a base station to the mobile stations, which in turn use these pseudorange correction values to correct their own location determinations. The mobile stations use the pseudorange correction values as a parameter to determine the encryption key for messages transmitted to other mobile stations.

Applicants note that the Examiner's characterization of Schipper is incorrect in several important respects. First, the pseudorange measurements are not the same as location data. Instead, the pseudorange measurements quantify distance or range between the station and the satellite. If four pseudorange measurements can be acquired from four different satellites, then location can be derived from the pseudorange measurements—but, the pseudorange measurements themselves do not identify location. In contrast, pseudorange correction values (PRC) represent mathematical corrections to pseudorange measurements and are obtained by comparing received pseudorange with expected pseudorange based on the known position of the fixed station. The PRC itself does not define a specific location; it merely specifies an offset. A location cannot be derived solely from a set of PRCs. Second, even if the PRC were construed as analogous to location data, the same PRC is used to determine the encryption key for plural mobile stations. Thus, it does not uniquely identify a specific geographic location and would not serve the purpose of the present invention of permitting access to the digital information only at the specific geographic

location. As with the other references, Schipper fails to suggest or disclose any claim of the present application.

Fennel, Jr. et al. discloses an encryption system based on channel destination addresses for a time division multiple access (TDMA) satellite communication network. Specifically, Fennel, Jr. uses a channel destination address (e.g., 1, 2, 3, ...) for encryption. These addresses are merely code designations for the stations, and do not contain any information that identifies specific geographic locations. It should be understood that an encryption system using these channel addresses would be unable to enforce access to the encrypted digital information only at a specific geographic location. Indeed, a station located anywhere would be able to recover the information as long as the channel address were known. Fennel, Jr. fails to suggest or disclose any claim of the patent application.

Hastings discloses information files stored in encrypted form on a CD-ROM. The same CD-ROM also contains a list of authorized geographic regions and decryption key files. A table (see, e.g., Table 1) links the encrypted files, the decryption keys necessary to decrypt the encrypted files, and the associated geographic regions in which the keys can be accessed. The computer system includes a GPS receiver, which provides current location information. To operate the system, a user first enters a password. If the password is authentic, the computer compares the location information obtained using the GPS receiver with the list of authorized geographic regions defined in the table. If there is a match, the computer system retrieves the corresponding decryption key from the CD-ROM and uses the key to decrypt the encrypted file authorized for use in that geographic region, thereby enabling the user to access the decrypted file.

As with Shimada described above, Hastings uses location information to determine whether to enable access to stored decryption keys that can decrypt digital information, but there is nothing inherent in the digital information itself that prevents it from being accessed anywhere but the desired location. Hastings uses location

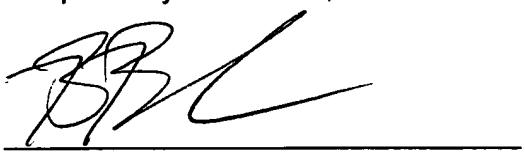
information as a form of gate keeper process, in contrast to the present invention in which the digital information is encrypted using a key based on location data. Hastings therefore fails to make up for the significant deficiency of Shimada, and the proposed combination of references thereby fails to suggest or disclose the claims as set forth above.

Emery discloses a method for linking telephone numbers and identifiers with geographic location. The reference has no applicability to the present invention and fails to make up for the deficiencies of Shimada discussed above.

In view of the foregoing, Applicants respectfully submit that Claims 55-91 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,



Date: May 27, 2005

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000